SÄFFLE KOMMUN

Beslutad av: Kommunfullmäktige
Revideras av: Kommunledningskontoret

POLICY

Datum
2022-09-05

Beteckning/dnr
KS/2022:226

Giltighetstid
Tillsvidare

Utgåva
1

Tillämpningsområde
Säffle kommunkoncern

Policy för informationssäkerhet

Innehåll

1 Bakgrund

Information är en av kommunens viktigaste tillgångar och hanteringen av den är en viktig och naturlig del i alla verksamheters dagliga arbete, samt en förutsättning för digitalisering och för att verksamheterna ska nå sina mål.

Att informationen som kommunen hanterar i kontakt med kommuninvånare, företag, organisationer och även inom vår egen organisation är korrekt utgör en grund för tillit och förtroende. Det är även viktigt att informationen är tillgänglig när den behövs och att känslig information skyddas för att vi ska kunna fullgöra vårt uppdrag.

Arbetet med informationssäkerhet ska vara långsiktigt och kontinuerligt, omfatta alla delar av kommunens verksamheteter och alla de informationstillgångar som vi äger eller hanterar.

1.1 Syftet med policyn

Policyn utgör kommunkoncernens viljeinriktning för att hantera kommunkoncernens information på ett systematiskt och informationssäkert sätt.

1.2 Målgrupp

Policyn omfattar förtroendevalda, chefer, medarbetare och uppdragstagare inom Säffle kommunkoncern.

1.3 Övriga styrdokument, lagar och förordningar

- Dataskyddsförordningen
- Dataskyddslagen
- ISO 27000-serien
- Säkerhetsskyddslagen (2018:585)
- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS-direktivet)

1.4 Begreppsförklaring

Information
Information är enkelt uttryckt data som presenteras i ett sammanhang som tolkas av en mottagare. Information kan vara konkret (exempelvis en budget) eller vag och subjektiv (exempelvis en vision eller åsikter).

Informationstillgångar
Allt som innehåller information samt allt och alla som bär på information. T ex mobiltelefoner, verksamhetssystem och medarbetare.

Verksamhetssystem
System som insamlar, lagrar, bearbetar eller distribuerar och presenterar information.

Informationssäkerhet
Är den säkerhet som omfattar våra informationstillgångar och förmågan att upprätthålla önskad konfidentialitet, riktighet och tillgänglighet.

Konfidentiell
Innebär att informationen eller i vissa fall informationstillgången inte får nås eller avslöjas för någon obehörig.

Riktighet
Innebär att informationen inte får ändras av obehöriga, inte av misstag och inte på grund av en funktionsstörning.

Tillgänglighet
Innebär att informationen går att nyttjas av behörig användare vid behov.

LIS
Ledningssystem för informationssäkerhet. En metod för att arbeta övergripande och systematiskt med informationssäkerhet. Metoden bygger på standarderna i 27000-serien och rekommenderas av Myndigheten för samhällsskydd och beredskap (MSB).

2 Policy för informationssäkerhet

2.1 Ansvar, organisation och roller

Ansvaret för informationssäkerhet följer det ordinarie verksamhetsansvaret. Detta gäller från kommunledningen till den enskilde medarbetaren, och innebär att den som är ansvarig för en viss verksamhet också är ansvarig för informationssäkerheten inom verksamhetsområdet. Kommunkoncernens informationssäkerhetssamordnare och övriga som arbetar med dataskydd och informationssäkerhet fungerar som stöd till kommunkoncernens verksamheter i arbetet med att uppfylla informationssäkerhetsansvaret.

2.1.1 Organisation

Kommunfullmäktige uttrycker sin viljeinriktning rörande kommunens arbete med informationssäkerhet i denna policy.

Kommunstyrelsen ansvarar för att samordna och följa upp kommunens informationssäkerhetsarbete. Kommunstyrelsen har det övergripande ansvaret för att utarbeta, förvalta och följa upp riktlinjer för informationssäkerhet.

Nämnderna och styrelserna ansvarar för informationsägarskapet inom ramen för sina verksamheter. Informationsägaren har det yttersta ansvaret för sin information och avgör vilken information som får hanteras, hur den får hanteras och av vem den får hanteras.

Anställda, förtroendevalda och uppdragstagare ansvarar för att följa de informationssäkerhetsriktlinjer och instruktioner som finns samt att agera säkerhetsmedvetet.

2.1.2 Roller

Kommundirektören har det övergripande ansvaret för informationssäkerheten och att det finns en tydlig ansvarsfördelning för att upprätthålla säkerheten.

Personuppgiftsansvarig är den som bestämmer ändamålen för behandlingen av personuppgifter.

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvarigas organisation.

Informationsägaren äger och ansvarar för att informationen är riktig och tillförlitlig, samt för det sätt informationen sprids.

Systemägaren har det överordnade ansvaret för administration och drift av en eller flera informationstillgångar.

Systemförvaltaren har till skillnad från systemägaren det operativa ansvaret för en eller flera informationstillgångar. Systemförvaltaren utses av systemägaren.

Säkerhetsskyddschef ansvarar för informationssäkerheten i verksamhet som har betydelse för Sveriges säkerhet och lyder under säkerhetsskyddslagen.

Säkerhetssamordnare genomför säkerhetsanalyser på uppdrag av säkerhetsskyddschefen.

Dataskyddsombudets roll är att regelbundet utbilda, rådgöra och granska nämndens informationssäkerhet, med särskilt fokus på att granska efterlevnaden av dataskyddsförordningen.

Informationssäkerhetssamordnaren har det övergripande ansvaret för att leda, utveckla och samordna arbetet med informationssäkerhet i kommunen. Informationssäkerhetssamordnaren är en stödfunktion för ledning och verksamheterna.

IT-chefen har det operativa ansvaret för att uppfylla de krav som verksamheten ställer på den tekniska IT-infrastrukturen. IT-chefen har ett särskilt ansvar för den tekniska IT-säkerheten.

Dataskydd- och informationssäkerhetssamordnare (DIS) ska vara utsedd för varje personuppgiftsansvarig i kommunen och ansvarar för att samordna arbetet med dataskydd och informationssäkerhet på den egna förvaltningen/bolaget.

2.2 Policy

- Information är värdefullt och ska skyddas efter behov. Ett bra informationssäkerhetsarbete är en förutsättning för effektiv och korrekt informationshantering. Detta skapar förtroende både inom och utanför organisationen.
- Informationssäkerhetsarbetet ska bedrivas systematiskt, formaliserat och riskorienterat.
- Informationssäkerhet är en grundförutsättning för att uppnå kvalitet och effektivitet i verksamheten, samt en förutsättning vid upphandling, digitalisering och mobilitet.
- Informationssäkerhetsarbetet ska skydda kommunens information genom tekniska och organisatoriska säkerhetsåtgärder, utifrån genomförda informationssäkerhetsklassificeringar och riskanalyser.
- Det ska finnas en organisation med tydlig fördelning av ansvar för informationstillgångar och med relevanta roller för ledning och genomförande av ett systematiskt informationssäkerhetsarbete
- Alla informationstillgångar ska ha en ägare. Informationsägaren ansvarar för klassificeringen av informationen och ställer de säkerhetskrav som behövs för att nå önskad säkerhet.
- Alla verksamhetssystem ska ha en systemägare som ansvarar för att säkerhetskraven på systemet uppfylls, och en systemförvaltare som ser till att åtgärder vidtas i aktuellt system för att uppnå detta.
- Chefer, medarbetare och förtroendevalda ska genomgå relevant utbildning inom informationssäkerhet.
- Det ska finnas en kultur som uppmuntrar engagemang hos alla medarbetare och, förutom att följa gemensamma riktlinjer och rutiner, motiverar dem att delta i att ständigt förbättra informationssäkerhetsarbetet.

3 Uppföljning och revidering

Nämnder och bolagsstyrelser ska årligen planera och följa upp informationssäkerhetsarbetet och vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig säkerhet.

Policyn för informationssäkerhet ska revideras vart fjärde år eller vid behov. I samband med revideringen ska tillhörande riktlinjer och rutiner revideras på motsvarande sätt.